REPLACEMENT SHEET

ABSTRACT

A traceable method for encrypting and/or decrypting data
broadcast by at least one transmitter towards several decoders
includes the steps: during encryption of broadcast data, the
transmitter implements (in 86) at least one first secret
function to transform an unencrypted message into an encrypted
message; and during decryption of the broadcast data, all the
decoders implement (in 92) at least one common second secret
function, each decoder using therefor a mathematical
description of the second function stored in a memory (21),
the mathematical description of the second function being
different from one decoder to another or from one group of
decoders to another such that the mathematical description
used identifies exclusively the particular decoder or group of
decoders.